UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; and Does 1-15, *Defendants*.	Civil Action No. **FILED UNDER SEAL**

DECLARATION OF LAURA HARRIS IN SUPPORT OF PLAINTIFF'S EX PARTE MOTION FOR A TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

I, Laura Harris, hereby declare and state as follows:

1. I am an attorney with the law firm of King & Spalding LLP and counsel of record for Plaintiff Google LLC ("Google"). I am a member of good standing of the bar of New York. I make this declaration in support of Google's Motion for an Emergency Ex Parte Temporary Restraining Order ("TRO Motion"). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. This Court may issue a temporary restraining order without notice to Defendants if "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b). I submit this declaration because Google has not provided Defendants with notice of the filing of this action or Google's TRO Motion for the reasons provided below. I certify that the necessity for this emergency hearing arises from the circumstances of this case and not from a lack of diligence on Google's part.

I. Basis For Ex Parte TRO Motion

3. Google seeks an Emergency Ex Parte Temporary Restraining Order to disrupt Defendants' operation of a far-reaching criminal enterprise (the "Glupteba Enterprise" or "Enterprise"), which exploits a botnet under the Enterprise's control to target consumers' personal devices, compromise the security of their accounts and sensitive personal information, disable their device security, sell access to their personal accounts, facilitate criminal activity by proxying it through the victims' malware-infected devices, and commit other malicious activity and cybercrimes.

4. As described in Google's TRO Motion and supporting documents, Defendants have created false advertising that triggers the download and installation of Glupteba malware onto personal devices, thereby duping users into inadvertently installing malware that hijacks their computers for exploitation by the Glupteba Enterprise. Declaration of Shane Huntley ("Huntley Decl.") ¶¶ 23–30.

5. The Glupteba Enterprise has infected approximately one million computers and internet-connected devices worldwide with its malware and continues to infect new devices every day, causing irreparable harm to Google and its users:

a. After being installed on users' personal devices, the Glupteba malware enables the Glupteba Enterprise to control and direct the devices to perform disruptive and criminal activities. *Id.* ¶¶ 27–30, 42–43.

b. The Glupteba Enterprise harvests users' sensitive, personal information stored on internet browsers and sells access to stolen accounts to third-party customers. *Id.* ¶¶ 44–54.

c. The Glupteba Enterprise sells credit cards to be used in ad fraud from a website called "Extracard.net." *Id.* ¶¶ 55–60.

d. The Glupteba Enterprise sells access to the IP addresses of infected devices to third-party customers. *Id.* ¶¶ 64–68. Many of those customers are cybercriminals themselves, and they use the IP addresses to proxy or relay their internet activity through the infected devices and evade detection from security systems that are designed to screen for suspicious IP addresses. *Id.* ¶ 64.

e. The Glupteba Enterprise operates a "cryptojacking" scheme that enables the Enterprise to mine cryptocurrency through infected devices, which insulates the Enterprise from incurring the electricity and computer-processing costs associated with doing so. *Id.* ¶¶ 73–76.

6. Certain IP addresses associated with web hosting companies have been identified as command and control servers for the Glupteba botnet and are set forth in Appendix A to the Complaint. A true and correct copy of that document is attached as **Appendix A** to the Complaint.

7. To disrupt the Glupteba botnet and the Enterprise behind it, Google has developed a disruption plan that seeks to shut down the domains used by the botnet and disable the servers the Enterprise uses to control it. Executing this disruption plan requires coordination with many different web hosting companies and other third parties, as well as law enforcement. It is critical to implement this plan without notice to the Defendants because, with notice, Defendants would simply move their infrastructure to new domains or servers, frustrating efforts to disrupt the botnet.

8. I have been informed that Google's Threat Analysis Group ("TAG") has attempted to identify the true identities of all responsible Defendants but has been unable to do so. Based on TAG's research, Defendants likely provided contact information to web hosting companies during the domain-name registration process, which could potentially include mailing addresses, email addresses, facsimile numbers, and telephone numbers that could identify additional defendants.

9. As counsel for Google, I am aware of previous cases in which federal district courts granted ex parte relief to disrupt similarly malicious botnet activity:

a. The Eastern District of New York issued an ex parte temporary restraining order and order to show cause to disrupt the "Necurs" botnet in *Microsoft Corp. v. John Does 1-2*, No. 1:20-cv-01217-LDH-RER (E.D.N.Y. 2020). A true and correct copy of the March 5, 2020 order is attached as **Exhibit 1**.

b. The Eastern District of New York issued an ex parte temporary restraining order and order to show cause to disrupt the "Dorkbot" botnet in *Microsoft Corp. v. John Does 1-5*, No. 1:15-cv-06565-NGG-LB (E.D.N.Y. 2015). A true and correct copy of the November 23, 2015 order is attached as **Exhibit 2**.

c. The Eastern District of New York issued an ex parte temporary restraining order and order to show cause to disrupt the "Zeus" botnet in *Microsoft Corp. v. John Does 1-39*, No. 1:12-cv-01335-SJ-RLM (E.D.N.Y. 2012). A true and correct copy of the March 19, 2012 order is attached as **Exhibit 3**.

d. In *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009), the Northern District of California issued an ex parte temporary restraining order and order to show cause to disrupt the defendant's alleged criminal activity, including its collaboration with "bot herders" to deploy botnets targeting thousands of personal devices. A true and correct copy of the June 2, 2009 order is attached as **Exhibit 4**.

e. Additional relevant precedent is set forth on pages 20 to 22 of Google's Memorandum of Law in Support of Its Motion for a Temporary Restraining Order and Order to Show Cause.

10. As discussed more fully in Google's accompanying TRO Motion, Google is likely to prevail on the merits of this case and hold the Glupteba Enterprise liable for its violations of federal law. Defendants are operating a worldwide criminal enterprise using technology that can be easily concealed and destroyed; they are relying on a botnet with a decentralized command-and-control system; and they have inflicted and are continuing to inflict harm on personal users and Google in the process. Without immediate, ex parte injunctive relief, Defendants will likely be able to evade any court-ordered efforts to disrupt the Glupteba Enterprise by destroying business records, modifying or destroying the Glupteba malware, relocating or dissipating assets, and otherwise concealing evidence of the Enterprise's malicious and criminal activity. For these reasons, there is good cause for this Court to grant the requested relief without providing advance notice to Defendants.

II. Notice and Service of Process To Defendants

11. On behalf of Google, King & Spalding plans to attempt to provide notice of the pleadings, TRO Application, and preliminary injunction hearing to Defendants in the following ways: (A) by serving notice of the pleadings and any TRO or preliminary injunction hearing to a physical address associated with Defendants; (B) by serving notice to email addresses associated with Defendants; (C) by serving notice and a link to the pleadings to Defendants through text message; and (D) by

undergoing the domain-name dispute resolution process offered by the Internet Corporation for Assigned Names and Numbers ("ICANN").

12. Defendants are all believed to reside in Russia. Although Russia is a party to the Hague Convention on the Service Abroad of Judicial and Extra Judicial Documents, Russia has suspended all judicial cooperation with the United States. According to the State Department, "[t]he Russian Federation refuses to serve letters of request from the United States for service of process presented under the terms of the 1965 Hague Service Convention or to execute letters rogatory requesting service of process transmitted via diplomatic channels. The Russian Federation also declines to give consideration to U.S. requests to obtain evidence." U.S. Dep't of State, *Russia Judicial Assistance Information*, https://travel.state.gov/content/travel/en/legal/Judicial-Assistance-Country-Information/RussianFederation.html (last accessed Nov. 19, 2021). Moreover, "requests sent directly by litigants to the Russian Central Authority under the Hague Service Convention are returned unexecuted." *Id.* Service through the Hague Convention would be futile, and in any event is not required under Federal Rule of Civil Procedure 4(f). *First American Corp. v. Price Waterhouse LLP*, 154 F.3d 16, 21 (2d Cir. 1998) ("The Hague Convention is not the exclusive means for obtaining discovery from a foreign entity. Nor is the Convention necessarily the means of first resort.") (cleaned up); *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 377 (S.D.N.Y. 2018) ("[T]he rule does not require a party to serve process by the means specified in subsections 4(f)(1) and (f)(2) before a court permits alternative service by 'other means' under Rule 4(f)(3).").

A. Service to Physical Address Associated with Defendants.

13. King & Spalding will attempt to provide notice of any TRO and preliminary injunction hearing to Defendants on behalf of Google. King & Spalding will attempt to serve the Complaint to Defendants by sending the pleadings by express mail to a physical address in Russia believed to be used by the Defendants: 123112, Moscow, Presnenskaya Embankment 12, Office 5.

B. Service to Email Addresses Associated with Defendants.

14. King & Spalding will attempt to provide notice of any TRO and preliminary injunction hearing to Defendants on behalf of Google. King & Spalding will also attempt to serve the Complaint to Defendants by sending the pleadings to email addresses associated with Defendants or otherwise provided by Defendants to the internet domain registrars and IP address hosting companies, apart from those that may be affected by Google's disruption of Google Workspace accounts associated with Defendants.

C. Service by Text Message to Numbers Associated with Defendants.

15. King & Spalding will also attempt to provide notice of any TRO, preliminary injunction hearing, and service of the Complaint by sending a text message with a link to download the pleadings to phone numbers associated with the Defendants. In particular, texts will be sent to Alexander Filippov at +7 925 037-99-63 and +7 995 300-69-69, and to Dmitry Starovikov at +7 8 (903) 555-22-29.

D. Providing Notice through ICANN.

16. King & Spalding will also attempt to provide notice of the pleadings, along with any TRO or preliminary injunction hearing, to Defendants through

ICANN—a California non-profit partnership responsible for coordinating domain names and IP addresses worldwide. Among other things, ICANN operates an accreditation system for registrars, including by administering domain-name registration contracts.

17. ICANN sets forth a process for serving notice of a complaint relating to a registrant's domains pursuant to the ICANN Registrar Accreditation Agreement. A true and correct copy of the ICANN Registrar Accreditation Agreement is attached at **Exhibit 5**.

18. Section 3.7.7.1 of the Registrar Accreditation Agreement requires each domain "Registered Name Holder" to provide "accurate and reliable contact details," which includes: "the full name, postal address, email address, voice telephone number, and fax number if available of the Registered Name Holder." If the Registered Name Holder is an organization, association, or corporation, then they must also provide the "name of authorized person for contact purposes."

19. If the Registered Name Holder willfully provides inaccurate or unreliable information and fails to promptly update its contact information (or fails to respond for over 15 calendar days to inquiries about that information), then that "shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration." Registrar Accreditation Agreement § 3.7.7.2.

20. The Registrar Accreditation Agreement requires Registered Name Holders to abide by the Uniform Domain Name Dispute Resolution Policy ("UDRP"). *See id.* § 3.8. A true and correct copy of the UDRP is attached as **Exhibit 6**.

21. UDRP proceedings apply the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"). A true and correct copy of the Rules is attached at **Exhibit 7**.

22. An ICANN-approved dispute resolution service provider must "employ reasonably available means calculated to achieve actual notice" to the holder of a domain-name registration that is the subject of a complaint relating to the domain name. *See* Rules § 2(a). Under Section 2(a)(i) through (iii) of the Rules, a service provider may satisfy that responsibility through the following measures:

i. sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

ii. sending the complaint, including any annexes, in electronic form by email to:

A. the email addresses for those technical, administrative, and billing contacts;

B. postmaster@<the contested domain name>; and

C. if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any email address shown or email links on that web page; and

iii. sending the complaint, including any annexes, to any email address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other email addresses provided to the Provider by Complainant under Paragraph 3(b)(v)."

23. King & Spalding will accordingly attempt to notify Defendants of any TRO and preliminary injunction hearing (along with service of the Complaint) by sending ICANN copies of the applicable documents, thereby triggering ICANN's duty to provide actual notice of the dispute to the holders of the domain-name registrations associated with Defendants.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed on December 2, 2021 in New York, New York.

Laura Harris